UNCLAS SECTION 01 OF 10 NEW DELHI 007026

SIPDIS

SENSITIVE

STATE/PM FOR DAS KARA BUE
STATE/PM FOR MICHELE MARKOFF
DOD FOR OASD/NII TIM BLOECHL

E.O. 12958: N/A
TAGS: KCIP TINT PREL ECPS KCRM IN US
SUBJECT: INDO-US CYBERSECURITY FORUM PREPARATORY CONSULTATIONS IN NEW DELHI

REF: A. NEW DELHI 5577
¶B. NEW DELHI 6980

¶1. (SBU) Summary: On October 14-18, 2004, Department Senior Coordinator for International Critical Infrastructure Protection Policy Michele Markoff and DOD Director of International Information Assurance Programs Tim Bloechl participated in preparatory meetings with the GOI for the November 9-10 Cybersecurity Forum in Washington. Arvind Gupta, Joint Secretary, National Security Council Secretariat, and Commander Mukesh Saini, Deputy Director

SIPDIS
(Information Security), NSCS, hosted the consultations and will lead the GOI delegation. Discussions included the Cybersecurity Forum's (CSF's) overall structure; designating co-chairs and selecting agenda topics for the five working groups; industry participation; site visits; and training and capacity building. The director of India's Computer Emergency Response Team (CERT-In) briefed on his organization's capabilities. Markoff asked Gupta for GOI support for a US-drafted UNGA Resolution calling for all UN Member States to join the 24/7 Cybercrime Point of Contact Network, while Gupta and Saini shared their vision to "inculcate a culture of cybersecurity" in India's IT sector. End Summary.

Getting to Know You (Again)

¶2. (SBU) Noting the long interval since the CSF last convened in April 29-30, 2002, Joint Director Gupta welcomed Markoff and Bloechl, and noted that much has changed in the field of cybersecurity technology, in the US and India's cybersecurity organizations, and in India's technical capabilities. Markoff remarked on the successful ITAA-NASSCOM India-US Information Security Summit 2004, at which she delivered the closing keynote address. Both Washington and New Delhi emphasized the importance of including the perspectives of both software developers and clients. Markoff listed a few key industries that rely heavily on secure and reliable IT systems: banks, health care, utilities, and transportation. Observing that the issue of cybersecurity is no longer "in the weeds," she said it is now recognized as an important part of US-India interdependence that is larger than the IT sector.

WG1: Legal Cooperation and Law Enforcement

¶3. (SBU) Markoff began by listing topics the USG wants to discuss in the area of cybersecurity legal cooperation and law enforcement:

-- How the GOI is organized to fight cybercrime;
-- Updates on relevant legislation;
-- Any plans to facilitate a Mutual Legal Assistance Treaty for computer crime;
-- The Council of Europe model cybercrime legislation;
-- How Indian law enforcement agencies approach cybercrime investigations and prosecutions; and
-- If India participates in, or plans to participate in, the 24/7 Cybercrime Point of Contact Network.

¶4. (SBU) Arguing for the inclusion of intrusion detection of Indian infrastructure to the agenda, MHA Joint Secretary Renuka Muttoo recalled a recent incident in which an American criminal/hacker allegedly misused an Indian proxy server to engage in credit card fraud and the printing of fraudulent certificates. Noting that the incident was reported to the US DOJ, she asked how such reporting could be institutionalized. Markoff indicated that the 24/7 Cybercrime Point of Contact Network, of which India was already a member, was the conduit for cyber crime reporting. Muttoo appeared unfamiliar with the 24/7 POC cybercrime network and Markoff promised to provide the name of the GOI contact. (NOTE: Embassy later passed GOI contact information via MEA.)

¶5. (SBU) Gupta queried whether this 24/7 network would be

used to report all cyber incidents. Markoff indicated that the U.S. has set up two separate 24/7 POCs -- one for watch and warning information sharing (US-CERT/NCSD), the other for law enforcement cooperation (DOJ) -- as a more effective way to ensure that information flows between professionals who understand each others priorities. Of course, the US and Indian CERTs would also pass crime-relevant information to appropriate law enforcement contacts within their respective countries should they receive it.

¶6. (SBU) Gupta indicated that the U.S. had not been responsive to all past bilateral requests for law enforcement cooperation. Markoff suggested that Gupta supply a list of unanswered requests. It would be useful for the CSF to review India's status in cybercrime substantive law (what activities are criminalized) as well as cybercrime procedural law (how far Indian authorities are allowed to cooperate on cross-border incidents). As an example, Markoff described a possible intrusion that could be routed through servers in several countries; in trying to trace back an attack, any gap in bilateral cybercrime cooperation would stop the investigation dead in its tracks.

¶7. (SBU) Gupta mentioned that the range of Indian law enforcement agencies with a potential role in cybercrime enforcement was larger than the delegation they could bring to the CSF, and offered to host a joint cybercrime law enforcement workshop in early 2005. He envisioned a two-day workshop that would look at problems and possible collaboration in cyber-forensics, mutual legal assistance, and computer-based investigation, noting that this could be another venue for private industry to join the government-to-government dialogue. Markoff responded that DOJ has participated in similar workshops, and suggested the proposal be discussed further at the CSF. Gupta said that the issue could also be pursued in the Law Enforcement Joint Working Group, and that the GOI Department of Information Technology had already held one working group on cyber law and cyber-crime.

¶8. (SBU) Gupta requested that DOJ brief on how high-tech crime is pursued, "from the start, conducting the investigation, through convictions, a complete walk-through" at the November CSF. Gupta's deputy, Commander Mukesh Saini, suggested that DOJ's Websnare Operation could be a useful case to profile.

WG2: Research and Development

¶9. (SBU) Markoff asked that India's Working Group 2 delegation report how New Delhi is poised for and can foster critical infrastructure protection research and development, outreach to industry and academia on CIP, and what cybersecurity issues the GOI sought to underline. She told Gupta that the InfoSec Research Council prepared a "Hard Problems List" of the technical hurdles in cybersecurity that need to be overcome (NOTE: Embassy later delivered a copy of the "Hard Problems List" to Saini). Markoff suggested that the USG and the GOI might partner in resolving some of these problems.

¶10. (SBU) In response, Gupta asked if the India-US Science and Technology Forum, which began in March 2000, might be a more appropriate venue for new R&D workshops in cybersecurity. In such an eventuality, the S&TF could provide POCs for science collaboration in several research areas, such as systems-oriented research architecture for dependability and survivability, systems management/monitoring/control, human monitoring, authentication, communications protocols, network security, accountability, and foundational research (logical languages and tools to develop systems). The most promising areas, Gupta said, were in applying cryptography for authentication and privacy, language-based security (i.e. voice recognition), diverse redundancy, and catastrophe-resistant architecture.

¶11. (SBU) Department of Information Technology Senior Director S. Basu said that working-level GOI R&D interests are focused on cryptography and crypto-analysis, network systems security, security architecture, operating system security, vulnerability detection and monitoring, and cyber-forensics. He expressed interest in reviewing the "Hard Problems List." Basu added that proposed topics for collaboration could include cyber forensic tools, authentication, speaker (voice) recognition, cryptography, and quantum cryptography.

¶12. (SBU) Dr. G. Athithan of the Defense Research and Development Organization (DRDO)/Center for Artificial Intelligence and Robotics said that DRDO and DIT had been working on IT security for 3-4 years. They have access to software developers in Bangalore through the marriage of "government money and private sector brains," while critical tasks are handled by government-funded laboratories, which

also conduct field-testing. Athithan underlined the GOI desire for tools to help monitor network traffic and capture keywords. He remarked that intercepting and reading Internet-based e-mail (webmail) was a difficult problem, and that webmail was developed by an Indian programmer to sidestep firewalls because it was more difficult to detect. After Athithan expressed his interest in "carnivore" software (to allow law enforcement agencies to read intercepted e-mails) Markoff and Bloechl -- as well as Gupta and Saini -- steered the conversation toward possible cooperation on cracking packet header data and session information, and away from reading intercepted text. Athithan proffered additional GOI R&D priorities: intrusion detection, modeling statistically normal network behavior to create a baseline, hacker tracing, and, again, viewing electronic content, "to help infer the origin and identity of an attacker."

¶13. (SBU) Gupta suggested Internet traffic monitoring and database analysis as areas for possible cooperation, noting that the GOI wishes to be able to profile and summarize data and databases, as well as profiling online user sessions (e-mail traffic and clustered browsing) over multi-day periods. Gupta then asked how the US monitors Internet traffic. Markoff said that US law does not permit general monitoring of Internet traffic; instead, if there is evidence of a crime, a court order can permit law enforcement to investigate relevant e-mail traffic.

¶14. (SBU) Bloechl suggested that the defense cooperation working group could discuss the issue in a military context, and echoed Markoff's statement that the USG does not monitor content, instead focusing on analysis, such as the case of worms or viruses indicated by packet header data. He explained that there is a great need to avoid violating US law by collecting information on US persons outside of a sanctioned law enforcement investigation.

¶15. (SBU) Gupta shared that the GOI,s interest was not in reading the data itself, but in technology to warehouse and analyze it. The GOI was interested in unclassified technology, as classified data is handled under separate procedures. Athithan interjected that he was interested in R&D, not law enforcement, and that the technology would be deployed toward a watch and warning function that would be in place prior to any legal permissions being sought for attempted intrusion or attack. He restated his interests as summarizing and profiling data, traffic analysis, and cluster analysis; Gupta added that the Indo-US Counterterrorism Joint Working Group was the appropriate forum for tools that would support actionable intelligence, while Athithan pushed for the technology to implement watch, warning and emergency response functions, as well as handling and storing digital evidence.

WG3: Critical Infrastructure Protection

¶16. (SBU) Markoff told Gupta that the Acting Director of DHS's National Cyber Security Division, Andy Purdy, will co-chair the Third Working Group, and will lead on watch and warning issues. Its presentation will include an overview of the capabilities and activities of the US Computer Emergency Readiness Team (US-CERT, which NCSD oversees), its mandated mission, its watch-and-warning capabilities, and a review of its public/private/academic/international outreach and partnerships. The USG sought a reciprocal briefing on the capabilities and activities of India's CERT-In. The working group will also explore collaboration opportunities, and welcomed a discussion on the following issues:

-- How was CERT-In created?
-- What is its mandate?
-- What alert and advisory systems are in place?
-- Is CERT-In operating in a 24/7 capacity for emergency responses? If not, will it do so in the future?
-- What kinds of international outreach does CERT-In pursue?

¶17. (SBU) Markoff then listed some potential avenues for collaboration between the two CERTs:

-- Designating POCs for bilateral communications;
-- Coordinating on cybersecurity incident responses;
-- Partnering on hard issues such as attribution and software assurance;
-- Sharing watch and warning information;
-- Fostering international cooperation beyond the bilateral relationship; and
-- Technical training assistance.

Other possibilities include exchanges of periodic reports on global Internet status, including trends, vulnerabilities, and incidents.

¶18. (SBU) Markoff reported that the USG has been considering architecture for an incident alert and management system, and is consulting with other allies in this regard. The system

would need to have real-time warning capabilities. Because CERT-In is India's designated national CERT, the two teams could begin sharing basic cyber watch and warning information almost immediately, she added. Markoff explained that CERT-In must be the government's authorized CERT and be able to share reciprocal information with US-CERT on a 24/7 basis, to qualify for this level of partnership.

¶19. (SBU) CERT-In Operations Manager Anil Sagar briefly presented on CERT-In's capabilities. He stated that CERT-In is GOI funded, 24/7 capable, and provides both pull (website: http://www.cert-in.org.in) and push (e-mail) alert services. He confirmed that it is the GOI-designated national CERT for all computer security incidents, government and private-sector, and has been operating since January. In response to Markoff's query as to CERT-In's membership in any regional agreements, Sagar said that CERT-In Director Dr. KK Bajaj was at that time engaged in membership consultations for the Asia-Pacific CERT (APCERT). CERT-In,s "wish list," according to Sagar, includes:

-- Knowledge-sharing with US-CERT of any discovered operating systems or applications vulnerabilities,
-- Updates on viruses and worms in circulation;
-- Assistance in vulnerability analysis;
-- Capabilities of incident handling;
-- Traffic monitoring;
-- Intrusion trends and warnings;
-- Hacker profiling; and
-- Assistance in testing patches for upcoming software vulnerabilities (NOTE: Sagar explained that CERT-In tests commercially-available patches before posting them on their website, because, he explained, they are very careful about preserving CERT-In,s reputation and do not wish to be associated with faulty patches.)

¶20. (SBU) In exchange, Sagar said that CERT-In could share the following with US-CERT: best practices on systems hardening; co-development of security applications; and information-sharing on systems vulnerabilities information.

WG4: Defense Cooperation

¶21. (SBU) Bloechl explained that robust cybersecurity for the US Defense Department and the military is already in place, under the auspices of a four-star general at US Strategic Command. A Joint Task Force (JTF) was created in 1998 as the primary computer network defense organization for the Defense Department. Other agency and military CERTs report to it, and it works in parallel with the US-CERT under the Department of Homeland Security as its defense sector counterpart. Bloechl invited the Working Group 4 delegation to visit the CSF early and tour the JTF/Global Network Operations Center in Washington, at which time the two delegations could discuss common goals and objectives for bilateral cooperation. Of key importance, he stressed, is that any organization the DOD partners with must be able to protect the information on its own networks.

¶22. (SBU) Bloechl then asked about the status of India's military CERT -- whether it has 24/7 intrusion detection, an R&D budget, details about its network security and if the military uses simulation modeling to test the security, indicators and warning capability, and pre-attack warning capability. Saini responded that each service (Army, Navy, Air Force) currently maintains its own independent computer networks, each overseen by its own "semblance of a CERT." Over time Saini planned to "grow the existing CERTs until they are fully functioning," primarily by enlarging and training their staffs, a goal he hopes to reach by 2007. Not even the Integrated Defense Staff yet possesses an integrated network -- the stress is to have adequate security in place before linking networks even at the IDS level. Furthermore, beyond the three service networks, the military has only a relatively small number of separate, Internet-accessible workstations. Despite pressure from within the military to expand Internet access, especially leading to broadband access, Saini's preference was to do so only after the military CERTs are fully functioning.

¶23. (SBU) Commodore J Jena of India's Integrated Defense Staff, who introduced himself by saying that "cybersecurity is my main activity," said the need for an expanded awareness of cybersecurity within the Indian military's Intranets remained acute. He asked whether USG networks were secured with commercially-available products or were manufactured within the government. Bloechl responded that classified systems are secured by USG agencies, including the NSA. Jena then asked what algorithms US classified networks use, and how reliable they are considered to be. Bloechl took the question and will pass to appropriate US offices for potential future action.

¶24. (SBU) In exchange for US-funded cybersecurity training, Jena said the Indian military was prepared to share the

following with the US:

-- Counterterrorism/low intensity conflict training and expertise;
-- A mode to tap into India's pool of IT talent; and
-- Its share in a bilateral cyberwarning function.

¶25. (SBU) Jena asked about adding additional areas to the discussion agenda, such as using endochromatic radioactive material-embedded hardware and software for security, cyber deterrence, and how to test for and sanitize malicious code. Markoff and Bloechl answered that the key to deterrence is cracking the attribution problem. After Jena asked about hardening systems to withstand an electro-magnetic pulse and how to reconstitute after such an attack, Markoff advised that such issues might be better addressed in the CTJWG. Bloechl added that some elements in DOD might be looking at such problems, but not his office. Bloechl and Jena agreed that data in languages other than English posed a hard problem, one that Markoff said was recognized at the World Summit on the Information Society (WSIS).

WG5: Standards and Software Assurance

¶26. (SBU) Markoff opened discussion on Working Group 5 by stating that Dr. Ron Ross of NIST would provide the CSF with a high-level overview of NIST's guidelines on security standards; show how the standards have international applicability; and outline the benefits of ongoing collaboration. Dr. SL Sarnot (Director General, Standards/Testing/Quality Certification Directorate, Ministry of Communications and Information Technology) stated that he had held a prior discussion with Dr. Ross, on common criteria for software assurance, and that both sides of the working group should be able to work well together. The GOI would seek cooperation in implementing NIST assurance protocols, and Sarnot said the US document is more "elaborate" than India's current program. He also asked for assistance in assurance frameworks and training to implement the common framework.

A Role for Private Industry

¶27. (SBU) Markoff and Gupta agreed that if the private sector and industry associations participate in the CSF, they would be included in the plenaries and could make their own presentations in that venue. Markoff suggested that in addition to IT industry representation, IT clients and firms involved in critical infrastructure (banking, telecommunications, utilities, and transportation, for example) should be invited. The delegation need not be huge, but American firms want to engage with their Indian counterparts, to foster deeper relations, but with a government component as the framework to facilitate an industry-to-industry dialogue, she stated. Gupta replied that the 2004 NASSCOM-ITAA conference had set the stage, and cybersecurity awareness has risen dramatically since the 2002 CSF. Markoff observed that the private sector must be part of the solution, as states cannot legislate strong cybersecurity protections into existence.

¶28. (SBU) Gupta observed that once private firms realize how much business will be tied to firms that work in a secure environment, they might end up pressuring governments into action. A few years ago there was marked resistance to adopting the common criteria for software assurance, he said, but now "all objections are gone." Many firms are only now beginning to understand the difference between information technology and information security. Markoff replied that as more firms lose productivity and business through cyber-attacks, worms, viruses, etc., fewer will require convincing.

¶29. (SBU) Markoff said that US industry participation would be based in part on the Indian list. She also offered that there could be sector-based break-out sessions for the commercial delegates. Specifically, Markoff said US firms would like to have Indian companies like TATA, WIPRO, and InfoSys represented, as well as national universities and research laboratories. Gupta promised to forward an Indian private-sector list, but cautioned that if they were unable to form a good delegation, they may rely on CII or NASSCOM representatives who could then report back to their members.

¶30. (SBU) Markoff suggested a list of possible issues and topics that would interest private industry, and that private sector participants could brief on:

-- E-signatures;
-- Bilateral certification authority;
-- Security procedures;
-- Technical and language skills;
-- Outsourcing;
-- Business activity disruption/disaster recovery;

-- Help desk/call center operations;
-- E-security with handheld devices;
-- Cybercrime laws;
-- Enforcement of privacy laws/standards;
-- Data privacy (including why India does not need to adopt the EU Privacy Law);
-- Need to enforce IPR;
-- Data protection laws;
-- Online database protection;
-- Physical security, including biometrics and closed circuit monitoring;
-- GPS issues;
-- Public safety concerns;
-- Outreach to small and mid-sized firms; and
-- Protecting financial data.

Site Visits

¶31. (SBU) Markoff, Bloechl and Gupta agreed that appropriate site visits would be of great value. Bloechl suggested that the defense WG could visit the Joint Task Force on November 8, before the plenary. Markoff added that a visit to US-CERT could also be planned for some of the other working groups. Both parties agreed that site visits would take place on November 8, on the basis of a list of sites the Indian delegation would like to visit.

Training Requests and Funding

¶32. (SBU) The most important item on New Delhi's training agenda is capacity building, Gupta reported. He emphasized the desire for expert exchanges and hands-on, side-by-side training. Admitting that funding, scheduling, and logistics for sending Indian cybersecurity professionals to the US were issues that needed to be worked out, Gupta offered to host American cybersecurity experts "for three days, or two months, or more" at Indian cybersecurity facilities and classes. Markoff and Gupta agreed that this would be a good issue for the CSF working groups to firm up. When Gupta pressed for working exchanges and hands-on training for CERT-In personnel at US-CERT, or vice versa, Bloechl cautioned him that most of the military CERTs, operations are at the top secret level, though there might be opportunities to observe operations at lower classifications.

¶33. (SBU) The US and Indian delegations briefly reviewed the September 3 GOI request for cyber forensics training (Ref A). When Gupta asked about funding, Markoff responded that there were few options due to budget constraints. She remarked that there may be opportunities, however, and noted that INL had funded training in Mumbai in 2003, but there is no clear answer yet on USG funding for non-military cybersecurity training. Markoff, Bloechl, Saini and Jena discussed the possibilities and limitations of funding via IMET, FMS and the DOD CT Fellowship Program. Markoff reported that several military training facilities that offer the kinds of courses the GOI sought now qualify for IMET. Markoff also suggested that the Monterey Naval Postgraduate School could customize senior-level courses for GOI groups. ODC Maj. Greg Winston added that Mobile Training Teams were another option, which could be brought to India under defense cooperation programs. He added that some IT-related courses are now covered under IMET. Two important hurdles, however, were that India's total IMET allocation for 2005 will be $1.4 million, and that courses must be at least five weeks in duration. Both delegations agreed to continue the discussion in Washington.

Lobbying for 24/7 Cybercrime POC Resolution

¶34. (SBU) Markoff asked Gupta for GOI support for a US-drafted UNGA resolution calling for all UN Member States to join the 24/7 Cybercrime Point of Contact Network originally created by the G-8. She said it would be the fifth resolution on cybersecurity. Gupta reacted positively and asked for a copy of the draft resolution. (NOTE: Embassy forwarded the draft resolution via the MEA.)

GOI's Cybersecurity Vision

¶35. (SBU) Gupta's short-term vision for GOI,s cybersecurity posture is to have dedicated cybersecurity officers in all government sectors capable of handling all ministry-related aspects of cybersecurity, whether a cyber attack occurs within a ministry or in the private sector areas the ministry oversees. This platform would then grow to include a fully functioning CERT for each sector, with all reporting to and deriving training from CERT-In. Gupta acknowledged that a dearth of trained personnel was slowing progress, which was the impetus behind what he called "inculcating a culture of cybersecurity into the private sector," first by mandating a cybersecurity requirement in engineering college curricula.

Saini elaborated that he would like to see cybersecurity training represent 5 percent of education within the IT sector, up from his estimate of 0.01 percent, by 2008. Eventually, he hoped that every IT professional would consider cybersecurity to be part of his bailiwick. Saini acknowledged that this would represent a massive investment by both the government and private industry, and that it would have to be a joint effort and not two parallel tracks.

High-Level Policy Support

¶36. (SBU) Noting that cybersecurity enjoys high-level support from NSA Dixit, chairman of the National Information Board (NIB) which keeps cybersecurity as a top-level policy interest, Gupta described the NIB as "very big," comprising MEA, MHA, Finance, MOD, DIT, the economic sectoral ministries, and law enforcement agencies. It meets every three months.

Other Cybersecurity Relationships Pale In Comparison

¶37. (SBU) Gupta said that although cybersecurity is clearly an issue of international importance, the Indo-US CSF is New Delhi's only substantial bilateral cybersecurity relationship. There had been some efforts at cooperation with Canada and Israel, "but they never took off." He also dismissed GOI efforts to foment cybersecurity cooperation with Russia without elaborating on them.

CSF Framework

¶38. (SBU) Markoff and Gupta agreed on the following structure for the five working groups and their co-chairs as follows:

Working Group 1: Legal Cooperation and Law Enforcement. USG co-chair Anthony Teelucksingh (Computer Crime and Intellectual Property Section, DOJ), GOI co-chair Ms. Renuka Muttoo, Joint Director, Ministry of Home Affairs.

Working Group 2: Research and Development. USG co-chair Stan Riveles (Office of the S&T Advisor to the Secretary), GOI co-chair Dr. AK Chakravarti (Advisor, Department of Information Technology, Ministry of Communications and Information Technology) (NOTE: The GOI co-chair was later changed to Dr. N Sitaram, Director Defense Research and Development Organization (DRDO)/Center for Artificial Intelligence and Robotics (CAIR) END NOTE.).

Working Group 3: Critical Infrastructure Protection, Watch, Warning, and Emergency Response. USG co-chair Andy Purdy (DHS National Cyber Security Division), GOI co-chair Dr. KK Bajaj (Director/CERT-In). (NOTE: "Emergency Response" was added to working group name to facilitate Bajaj's participation. END NOTE.)

Working Group 4: Defense Cooperation. USG co-chair Tim Bloechl (DOD Director of International Information Assurance Programs), GOI co-chair Mr. SK Sharma (Joint Secretary, Ministry of Defense).

Working Group 5: Standards. USG co-chair Dr. Ron Ross (NIST), GOI co-chair Dr. SL Sarnot (Director General, Standards/Testing/Quality Certification Directorate, Ministry of Communications and Information Technology).

¶39. (SBU) The two-day government-to-government forum was tentatively agreed to be structured as follows:

-- 11/9 morning: A comprehensive plenary session with all delegates attending. Working groups give short presentations of key challenges and accomplishments in their fields.
-- 11/9 afternoon: Plenary continues. Working groups continue their briefings.
-- 11/10 morning: Working groups break out into separate meetings.
-- 11/10 afternoon: Plenary reconvenes for lunch. Working groups report progress and road maps outlining next steps. Prepare joint statement.

USG Participants

¶40. (SBU) The following USG personnel participated in the preparatory consultations:

Michele Markoff, Senior Coordinator for International Critical Infrastructure Protection Policy, State/PM
Tim Bloechl, Director of International Information Assurance Programs, DOD
Linda Hall, US Embassy New Delhi, ORA
Howard Madnick, US Embassy New Delhi, POL
Maj. Greg Winston, US Embassy New Delhi, ODC

GOI Participants

¶41. (SBU) The following GOI officials participated in the preparatory consultations:

Arvind Gupta, Joint Secretary, NSCS (Ref B)
Commander Mukesh Saini, Deputy Director (Information Security), NSCS (Ref B)
Rajesh Mohan, Joint Director, National Security Council Secretariat

SIPDIS
Commodore J Jena, HQ Integrated Defense Staff/DACIDS (Information Warfare/Information Technology)
Renuka Muttoo, Joint Director, Ministry of Home Affairs
Dr. G Athithan, Defense Research and Development Organization (DRDO)/Center for Artificial Intelligence and Robotics
Dr. SL Sarnot, Director General Standards/Testing/Quality Certification Directorate, Ministry of Communications and Information Technology, Department of Information Technology
S Basu, Senior Director, DIT
ASA Krishnan, Director R&D, DIT
Anil Sagar, Operations Manager, CERT-In
Sabyasachi Chakrabarty, Scientist B, CERT-In, DIT

¶42. (U) Senior Coordinator Michele Markoff cleared this message.
MULFORD